Crypto FAQ
CryptoBytes
RSA Algorithm
PKCS
Advanced Encryption Standard
Tech Notes
Staff & Associates
Standards
Bulletins
Challenges

# Markus Jakobsson

***Full Publication List***

- P. Golle, M. Jakobsson, A. Juels, P. Syverson, "Universal Re-encryption for Mixnets", RSA-CT '04 (pdf)
- P. Golle, M. Jakobsson, "Reusable Anonymous Return Channels", WPES '03 (pdf)
- M. Jakobsson, S. Wetzel, B. Yener, "Stealth Attacks on Ad-Hoc Wireless Networks", IEEE VTC '03 (pdf)
- M. Jakobsson, F. Menczer, "Untraceable Email Cluster Bombs: On Agent-Based Distributed Denial of Service'
- M. Jakobsson, J. Linn, J. Algesheimer, "How to Protect Against a Militant Spammer" (ps, pdf)
- N. Ben Salem, L. Buttyan, J.-P. Hubaux, M. Jakobsson, "A Charging and Rewarding Scheme for Packet Forwa hop Cellular Networks", ACM MobiHoc '03 (ps,pdf)
- M. Jakobsson, J.-P.Hubaux and L. Buttyan, "A Micro-Payment Scheme Encouraging Collaboration in Multi-Ho Networks", FC '03 (ps,pdf)
- M. Jakobsson, T. Leighton, S. Micali and M. Szydlo, "Fractal Merkle Tree Representation and Traversal", RSA
- A. Boldyreva, M Jakobsson, "Theft protected proprietary certificates", DRM '02 (ps,pdf)
- P. Golle, S. Zhong, M. Jakobsson, A. Juels, D. Boneh,"Optimistic Mixing for Exit-Polls", Asiacrypt '02. (pdf)
- P. MacKenzie, T. Shrimpton, M. Jakobsson, "Threshold Password-Authenticated Key Exchange", Crypto '02. (
- M. Jakobsson, "Fractal Hash Sequence Representation and Traversal", ISIT '02. (ps,pdf,code). One-page abs
- M. Jakobsson, A. Juels, R. Rivest, "Making Mix Nets Robust For Electronic Voting By Randomized Partial Che
- D. Coppersmith, M. Jakobsson, "Almost Optimal Hash Sequence Traversal", FC '02 (ps, pdf,code)
- M. Jakobsson, "Financial Instruments in Recommendation Mechanisms", FC '02 (ps, pdf)
- J. Garay, M. Jakobsson, "Timed Release of Standard Digital Signatures", FC '02 (ps, pdf)
- F. Menczer, N. Street, N. Vishwakarma, A. Monge, M. Jakobsson, "Intellishopper: A Proactive, Personal, Priva Assistant", AAMAS '02
- M. Jakobsson, M. Reiter, "Discouraging Software Piracy Using Software Aging", WSPDRM '01. (ps,pdf)
- M. Jakobsson, A. Juels. P. Nguyen, "Proprietary Certificates", RSA '02 . (ps,pdf)
- M. Jakobsson, A. Juels, "An Optimally Robust Hybrid Mix Network", PODC '01 (ps,pdf)
- M. Jakobsson, S. Wetzel, "Security Weaknesses in Bluetooth", RSA '01. (ps,pdf,ref)
- M. Jakobsson, D. Pointcheval, "Mutual Authentication for Low-Power Mobile Devices," Financial Crypto '01. (p
- M. Jakobsson, D. Pointcheval, A. Young, "Secure Mobile Gambling," RSA '01. (ps,pdf,ref)
- M. Jakobsson, A. Juels, "Addition of ElGamal Plaintexts," Asiacrypt '00. (ps,pdf,ref)
- M. Jakobsson, A. Juels, "Mix and Match: Secure Function Evaluation via Ciphertexts," Asiacrypt '00. (ps,pdf)
- R. Arlein, B. Jai, M. Jakobsson, F. Monrose, M. Reiter, "Privacy-Preserving Global Customization," ACM E-Co (pdf,ref)
- C.-P. Schnorr, M. Jakobsson, "Security of Signed ElGamal Encryption," Asiacrypt '00. (ps,pdf,ref)
- M. Jakobsson, A. Juels, E. Shriver, B. Hillyer, "How To Turn Loaded Dice Into Fair Coins," IEEE Transactions Theory, May '00. (ps,pdf)
- P. Bohannon, M. Jakobsson, S. Srikwan, "Cryptographic Approaches to Privacy in Forensic DNA Databases," Cryptography '00. (ps,pdf)
- J. Garay, M. Jakobsson, P. MacKenzie, "Abuse-free Optimistic Contract Signing", Crypto '99. (ps,pdf,ref)
- M. Jakobsson, "Flash Mixing", PODC '99. (ps,pdf,ref) — considered
- G. Di Crescenzo, N. Ferguson, R. Impagliazzo, M. Jakobsson, "How To Forget a Secret", STACS '99. (ps,pdf)
- M. Jakobsson, D. M'Raihi, Y. Tsiounis, M. Yung, "Electronic payments: where do we go from here?," Invited ta (ps,pdf)
- C.P. Schnorr, M. Jakobsson, "Security of discrete log cryptosystems in the random oracle and generic model"
- M. Jakobsson, A. Juels, "Millimix: Mixing in Small Batches," DIMACS Technical Report 99-33. (ps,pdf)
- M. Jakobsson, A. Juels, "Proofs of Work and Breadpudding Protocols," CMS '99. (ps,pdf)
- M. Jakobsson, "Efficient Oblivious Proofs of Correct Exponentiation," CMS '99. (ps,pdf) — considered
- M. Jakobsson, P. MacKenzie, J.P. Stern, "Secure and Lightweight Advertising on the Web," WWW8 '99, Jourr Networks. (ps,pdf)
- M. Jakobsson, J.P. Stern, M. Yung, "Scramble All, Encrypt Small," Fast Software Encryption '99. (ps,pdf)
- M. Jakobsson, J. Mueller, "Improved Magic Ink Signatures Using Hints," Financial Crypto '99. (ps,pdf)
- M. Jakobsson, "Mini-Cash: A Minimalistic Approach to E-Commerce," Public Key Cryptography '99. (ps,pdf)
- M. Jakobsson, "On Quorum Controlled Asymmetric Proxy Re-encryption," Public Key Cryptography '99. (ps,pc
- M. Jakobsson, A. Juels, "X-Cash: Executable Digital Cash", Financial Cryptography '98. (ps,pdf)
- M. Jakobsson, E. Shriver, B. Hillyer, A. Juels, "A Practical Secure Physical Random Bit Generator," ACM Secu
- M. Jakobsson, D. M'Raihi, "Mix-based Electronic Payments," SAC '98. (ps,pdf)
- M. Jakobsson, "A Practical Mix," Eurocrypt '98. (ps,pdf,ref)
- M. Jakobsson, M. Yung, "On Assurance Structures for WWW Commerce," Financial Cryptography '98. (ps,pdf
- E. Gabber, M. Jakobsson, Y. Matias, A. Mayer, "Curbing Junk E-Mail via Secure Classification," Financial Cryp (ps,pdf)
- M. Jakobsson, "Privacy vs. Authenticity", PhD Thesis, University of California at San Diego '97. (ps,pdf)
- M. Jakobsson, M. Yung, "Distributed Magic Ink DSS Signatures", Eurocrypt '97. (ps,pdf)
- M. Jakobsson, M. Yung, "Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System," Finan (ps,pdf)
- A. Herzfeld, M. Jakobsson, S. Jarecki, H. Krawczyk, M. Yung, "Proactive Public Key and Signature Systems", '97. (ps,pdf)
- M. Bellare, M. Jakobsson, M. Yung, "Round-Optimal ZK Arguments based on any One-Way Function," Eurocr
- M. Jakobsson, M. Yung, "Proving Without Knowing", Crypto '96. (ps,pdf)

considered

- M. Jakobsson, K. Sako, R. Impagliazzo, "Designated Verifier Proofs and Their Applications", Eurocrypt '96. (ps
- M. Jakobsson, M. Yung, "Revokable and Versatile Electronic Money," ACM Security '96. (ps,pdf)
- M. Jakobsson, "Ripping Coins for a Fair Exchange," Eurocrypt '95. (ps,pdf)
- M. Jakobsson, "Blackmailing using Undeniable Signatures," Eurocrypt '94. (ps,pdf)
- M. Jakobsson, "Reducing costs in identification protocols," Rump session, Crypto '92. (ps,pdf)
- M. Jakobsson, "Machine-Generated Music with Themes", International Conference on Artificial Neural Networ
- G. Jakobsson, M. Jakobsson, M. Persson, "NO till vardags," ISBN 91 88070 14 X.

***Patent publications** (issued as of Sep 6 '03)*

| | |
|---|---|
| 6,598,163 | Flash mixing apparatus and method |
| 6,587,946 | Method and system for quorum controlled asymmetric proxy encryption |
| 6,574,658 | System and method for secure classification of electronic mail |
| 6,574,455 | Method and apparatus for ensuring security of users of bluetooth TM-enabled devices |
| 6,529,884 | Minimalistic electronic commerce system |
| 6,507,656 | Non malleable encryption apparatus and method |
| 6,501,380 | Probabilistic theft deterrence |
| 6,393,447 | Method and apparatus for extracting unbiased random bits from a potentially biased source of randomr |
| 6,317,833 | Practical mix-based election scheme |
| 6,317,499 | Storage device random bit generator |
| 6,157,920 | Executable digital cash for electronic commerce |
| 6,049,613 | Method and apparatus for encrypting, decrypting, and providing privacy for data values |

United States: 1-877-RSA-4900 or 781 515 5000, Europe, Middle East, Africa: +44 (0)1344 781000,
Asia/Pacific: + 61 2 9463 8400, Japan: +81 3 5222 5200